REMARKS

This Amendment is submitted in response to the Examiner's Action mailed September 12, 2005, with a shortened statutory period of three months set to expire December 12, 2005. Claims 1-3, 5-14, 16-21, 23-33, and 35-50 are currently pending.

The Examiner included a heading in the Action that reads "Claim Rejections – 35 U.S.C. § 112". Under this heading, the Examiner included a quotation of the first paragraph of 35 U.S.C. § 112. The Examiner then rejected claims 1-3, 5-14, 16-21, 23-33, and 35-50 under U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. However, no explanation whatsoever is provided by the Examiner of the deficiency of these claims. Applicants are unable to respond to this rejection because the Examiner has provided no explanation of the deficiency of the claims. Further, Applicants believe this rejection should be withdrawn because the Examiner has not described any deficiency of these claims.

The Examiner rejected claims 1-3, 5-14, 16-21, 23-33, and 35-50 under U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Specifically, the Examiner stated that the limitation "the client being incapable of decrypting the encrypted data" has no support in the specification.

The specification states that the server contacts the storage device directly. See specification page 7, lines 11-14. The server sends the data over the communications channel directly to the network storage device 108. See specification page 7, lines 11-14. Figure 3 depicts the operation of a secure sockets layer (SSL) communication between the storage device and the server. An SSL connection is maintained between the storage device and the server. See specification page 11, lines 13-16. SSL relies on public key cryptography. See specification page 11, line 29. "In a public key cryptosystem, the parties exchange public keys, but keep the private keys secret. In this way, each of the parties can encrypt messages to send to the other party, and only the intended recipient will be able to decrypt the message." Specification page 12, lines 6-10.

Applicants' specification explicitly states that only the parties that have possession of the keys can decrypt messages that were encrypted using these keys. See

specification page 12, lines 6-10. The server and storage device use SSL to communicate. Thus, Applicants' specification teaches that only the server and storage device can decrypt encrypted data that is transmitted between the server and storage device using SSL where only the server and storage device have possession of the keys used to encrypt the data. Because the client is not the intended recipient, the client is incapable of decrypting encrypted data that is transmitted between the server and storage device because the client is not in possession of the keys. Therefore, Applicants' specification complies with the written description requirement because the limitation "the client being incapable of decrypting the encrypted data" is supported in the specification.

The Examiner rejected claims 1-3, 5-14, 16-21, 23-33, and 35-50 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 6,005,939 issued to *Fortenberry*. This rejection, as it might be applied to the claims as amended, is respectfully traversed.

The Examiner stated that, for purposes of examination, the Examiner considered the limitation of "the client being incapable of decrypting the encrypted data" as corresponding to "a client not being able to decrypt an encrypted data unless the client possesses the decryption key".

Applicants' claim 1 is exemplary of the other independent claims. Applicants' claim 1 describes receiving from a client a request to transmit the data, encrypting the data, and transmitting the encrypted data to a storage device, that is associated with the client, connected to the network, the client being incapable of decrypting the encrypted data, wherein unencrypted transmission of the data through the client is bypassed. Applicants do not refer to any key in the claims. Applicants claim "the client being incapable of decrypting the encrypted data" in the independent claims. Applicants' claimed feature does not correspond to "a client not being able to decrypt an encrypted data unless the client possesses the decryption key".

The Examiner also stated that "applicant's passing the unencrypted transmission corresponds to transmission of the encrypted data between the two entities using a secure channel of communication". Applicants claim "wherein unencrypted transmission of the data through the client is bypassed". This means that an unencrypted transmission of the data does not occur through the client. This is not at all the same as transmitting

encrypted data between two entities using a secure channel of communication. Applicants refer to specific "data" in this feature. This is the data that was encrypted and then transmitted to a storage device that is associated with the client and connected to the network. Applicants do not claim merely encrypted transmissions using a secure channel of communication.

Further, just because unencrypted transmission is bypassed does not mean that two entities are communicating using a secure channel of communication. The Examiner has interpreted Applicants claims by substituting completely different concepts for the wording of Applicants claims which has fundamentally changed the meaning of the claimed feature.

The Examiner states that column 6, lines 16-46, of *Fortenberry* teaches "the client being incapable of decrypting the encrypted data". The cited section of *Fortenberry* teaches the user requesting that the passport agent release specific user information to the web site. This request is then encrypted. The passport agent is provided with a key with which to decrypt the encrypted message sent by the user. The user can decrypt the encrypted message that includes the request because it is the user that encrypted the message.

This section also describes the passport agent transmitting encrypted data to the web site. The user can decrypt the encrypted data because *Fortenberry* states at lines 26-29, "user 208 has previously provided to web site 210 a public key with which web site 210 can decode the encrypted data provided by passport agent". The user can decrypt the encrypted data because the user is the one that provided the key to use to decrypt the encrypted data.

Fortenberry states at lines 30-36, "the web site 210 receives the encrypted user information (i.e. the passport) from passport agent 216 and unlocks the message using the public key provided by the user 208". The user can decrypt the encrypted user information because the user is the one that provided the key to use to decrypt the encrypted user information.

Fortenberry further emphasizes, at lines 36-38, that it is the user, Applicants' client according to the Examiner, that can decrypt the encrypted information by stating

that "user 208 can provide to web site 210 one of several public keys which allow web site 210 to unlock data having one of several security levels".

The section cited by the Examiner, column 6, lines 16-46, states that it is the user that provides the key to decrypt the encrypted data. The user is able to decrypt the data because the user has the key. Therefore, the section cited by the Examiner teaches that the user is capable of decrypting the encrypted data. Therefore, *Fortenberry* does not anticipate Applicants' claims.

As discussed above, the Examiner again stated in this Action that the Examiner considers the "user" taught by *Fortenberry* as corresponding to Applicants' "client". The "user" taught by *Fortenberry* is capable of decrypting the encrypted information. Therefore, *Fortenberry* does not anticipate Applicants' claims.

Fortenberry teaches a user sending a request to a passport agent. The passport agent then transmits information about that user to a web site. The request from the user to the passport is encrypted. Before the passport agent sends the information about the user to the web site, the passport agent encrypts the information. The passport agent then sends encrypted data to the web site. The user provides a key to the web site for the web site to use to decrypt the information. Thus, the user is capable of decrypting the encrypted information because the user holds the key that is needed in order to be able to decrypt the encrypted data.

Applicants claim the storage device being associated with the client. In *Fortenberry*, the web site is not associated with the user. In fact, *Fortenberry* teaches away from the web site being associated with the user because according to *Fortenberry*, the user wishes to keep the user's identity secret from the web site. See column 2, lines 17-20. Since *Fortenberry* does not teach the web site being associated with the user, *Fortenberry* does not anticipate Applicants' claims.

Further, *Fortenberry* would not be properly combined with other art because *Fortenberry* teaches away from Applicants' claims. Applicants claim the client being incapable of decrypting the encrypted data wherein unencrypted transmissions of the data through the client is bypassed. *Fortenberry* teaches a passport agent that transmits encrypted data to the web site. The passport agent encrypts the data. The passport agent assigns an encryption key based on the user's password. The password agent then

provides the public key to the user. This public key is required in order to be able to decrypt the encrypted data.

The user then provides the web site with this key for the web site to use to decrypt the encrypted data. Thus, *Fortenberry* teaches the user being able to decrypt the encrypted data that is transmitted from the passport agent to the web site because the user provides the key to use for decryption. If the user has not provided the proper key for the web site to use to decrypt the data, the web site will not be able to decrypt the data. Therefore, *Fortenberry* does not teach the client being incapable of decrypting the encrypted data. *Fortenberry* expressly teaches the user being able to decrypt the data. Because *Fortenberry* does not teach the client being incapable of decrypting the encrypted data, *Fortenberry* does not anticipate Applicants' claims.

The remaining claims depend from the independent claims the storage device being associated with the client and the client being incapable of decrypting the encrypted data. Thus, the remaining claims are believed to be patentable because *Fortenberry* does not teach the features of the dependent claims in combination with the storage device being associated with the client and the client being incapable of decrypting the encrypted data.

For the reasons given above, *Fortenberry* does not anticipate Applicants' claims. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 11.14.05

Respectfully submitted,

Lisa L.B. Yociss
Reg. No. 36,975
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants